Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

News and Notes

Richard Gary Epstein, West Chester University of Pennsylvania, *Member IEEE*

Abstract – This paper describes the author's undergraduate Introduction to Computer Security and Ethics course. The main focus of this paper, beyond providing an overview of the course, is on how events in the news impact the course content. It also describes the author's efforts to motivate students to pay attention to current events and to understand the importance of developments in Information Assurance for our global culture. Two specific student assignments, relating to current events, are described.

Index terms – Integrating Information Assurance topics into the undergraduate curriculum, ethics, social implications, scenarios

I. INTRODUCTION

The author teaches an undergraduate course which serves as an introduction to computer security and ethics for undergraduate students who are either majoring in Computer Science or pursuing a minor in Information Technology. The ethics materials are intended to assure that our Computer Science curriculum is consistent with ABET (Accreditation Board for Engineering and Technology) requirements in terms of covering issues in computer ethics and the social implications of computing. The computer security materials serve as an introduction to Information Assurance as covered in our certificate program in Computer Security (based upon guidelines provided by the NSA's National Training Standards for Information Systems Security). The basic prerequisite for this course is some background to introductory programming. For example, Computer Science majors are required to have had two Java programming courses before they take this course.

An important aspect of this course is to interweave the ethical issues with the security issues. A recurring pattern in the course is to

1. Introduce a topic in ethics (e.g., privacy)
2. Follow this up with a discussion of related security concerns (e.g., phishing, spam, identity theft)
3. Conclude with a discussion of technologies Computer Scientists and Information Technologists have proposed to address the security concerns (e.g., two factor authentication, anonymous Web browsing)

Since the author began teachings this course (around the turn of the millennium), he has found it interesting to integrate news items into the discussions. Sometimes the news items are recent events, maybe events that came into the news on the very day the author is teaching the class. At other times (and more frequently) he draws upon news items that might have come into the media a while back (say, a few months back, or even a few years). The emphasis in this paper is on the manner in which the news items contributes to the course, the messages communicated by these news items, and some new assignments the author has integrated into his course for the first time this semester, assignments which encourage students to pay attention to unfolding news in the domain of Information Assurance.

This paper begins with an overview of the course (Section II). Then, we will discuss how news items are incorporated into the class discussions (Section III). Then, we will discuss the new assignments that the author is using for the first time this semester that aim to encourage students to become more aware of ongoing events in the realm of Information Assurance (Section IV).

II. OVERVIEW OF THE COURSE

This section presents an overview of the materials covered in the course. Some of the materials are provided via lecture notes and PowerPoint slides made available to the students via Blackboard. The introductory materials and the materials that relate to privacy, intellectual property, computer crime (what the author calls "nasty stuff"), information warfare and cryptography are of this nature. The remaining materials are provided in the coursepack for the course. The coursepack is not a printed document but rather a collection of articles that students can access freely from the ACM and IEEE Computer Society digital libraries. Indeed, the bulk of the reading materials for this course come from IEEE Security and Privacy, Communications of the ACM, IEEE Computer, IEEE IT Professional, and IEEE Spectrum.

All of the references cited in this paper from the above publications are in the coursepack. In many cases, in order to improve the reader-friendliness of this paper, the author just gives the reference number for the coursepack article being cited (e.g., [4]), leaving out the names of the

author or authors. The complete author and publication information for each reference will be found in the references section of this paper (Section VI).

The introductory lectures for this course provide an introduction to the basic ideas and terminology of computer security. These lectures give a general introduction to computer crime and hacking culture. The introductory lectures feature some interviews with experts who have studied the psychology of hacking, including interviews with Sarah Gordon and Charles Palmer. We also discuss the increasing importance of organized crime in the realm of computer crime. The introductory lectures include an overview of data from the CSI/FBI survey [1] and the trends that this survey sees in the area of computer security. These classes end with several in-class exercises that involve presenting students with a long list of information assets (most of them personal, some for a pretend company) and asking students to analyze the consequences of the threats of (1) interruption, (2) interception, (3) modification, and (4) fabrication for these assets.

The course then moves on to a discussion of privacy. This starts with an introduction to privacy, mostly from an ethical perspective. The privacy lecture notes discuss important privacy issues and threats and are very much influenced by the computer ethics book by Tavani [2]. We then move on to a discussion of tools developed by technologists to enforce privacy policies or to protect privacy. These include a discussion of P3P [3], followed by a discussion of Crowds [4] and Tor [5]. Although Crowds is no longer an important player in protecting privacy, the Crowds paper provides ideas that will help students to understand the Tor technology more easily. Finally, we discuss workplace monitoring of e-mail communications and Web browsing and we discuss Internet use policies within organizations [6].

The next topic is "Nasty Stuff" (i.e., computer crime). The author presents PowerPoint slides that goe over many historical incidents relating to computer crime. We begin with a brief introduction to Kevin Mitnick and the idea of social engineering. We then move on to discuss a rather long list of important incidents and the individuals associated with those incidents. These include the Morris worm (Robert Morris), the Melissa Virus (David Smith) the Code Red Worm, the ILoveYou worm (Onel de Guzman), denial of service attacks (Mafia Boy), the Slammer Worm (Sven Jaschen), Botz4Sale (Jeanson James Ancheta), and the Blaster Worm (Jeffrey Lee Parsons, who wrote a version of this worm). The computer crime lectures then go on to a discussion of the nature of cybercrime (and what should be considered cybercrime). We conclude with a rather lengthy discussion of social engineering, re-enacting several scenarios found in Mitnick's book, The Art of Deception[7]. In addition, the coursepack contains some papers describing some of the incidents listed above (like the Melissa Virus [8], the Code Red Worm [9], and the Blaster Worm [10]) and the more recent Storm Worm [11].

Other articles in the coursepack that relate to computer crime and malware include an excellent discussion of the situation we are facing in terms of worms [12] and another more recent article about the new kinds of attacks (using code obfuscation and polymporphism) the worm authors are using to trick antivirus software [13]. The coursepack also includes an article about security problems in online games by Gary McGraw and Greg Hoglund that we don't really have time to discuss in class, but which the author believes that many students may find interesting [14].

The next portion of the course is entitled "Privacy and Nasty Stuff". Now that we have been exposed to ethical issues relating to privacy and to the nature of computer crime and malware, we move on to discuss how nasty stuff and privacy interact. We discuss articles about spam that emphasize proposed solutions to the problems (e.g., the paper by Pfleeger et al. [15]) and an interesting study by Galen Grimes about how compliance with the CAN-SPAM Act of 2003 actually decreased in the period following the passing of that law [16]. This section of the course then goes on to discuss phishing [17] and the threats posed by social networking sites [18] and spyware [19].

The course then moves on to a discussion of intellectual property, using our intellectual property lecture notes. These notes begin with a discussion of the ethical issues, drawing upon various resources, including the aforementioned book by Tavani [2] and the excellent book Blown to Bits by Hal Abelson, Ken Ledeen and Harry Lewis [20]. We introduce students to the technologies behind digital rights management (drawing upon Blown to Bits [20]) and then discuss some proposals by Computer Scientists about how software piracy can be prevented (using the article by Naumovich et al. [21].)

Next, we turn our attention to the weakest link: the desktop computer and the user interface. Articles used in this part of the coursepack include some really provocative papers by Thelander [22] (on the Great Wall Syndrome), Gyongyi and his co-author [23] (on Google bombing, what they call Web Spam), and Cybenko [24] (on cognitive hacking). The Great Wall Syndrome refers to the use of personal digital assistants (e.g., flash drives) and the dangers they pose for organizations. Google bombing refers to the technologies being developed to manipulate search engine results. Cognitive hacking refers to attempts by hackers to manipulate public perceptions using the Web. This section of the course

ends with a discussion of the psychology of users and how user psychology contributes to the weakest link (e.g., the paper by West [25]).

The next topic covered in the course is information warfare. The lecture notes draw upon Denning's book on information warfare [26] and various Web resources. The Web resources provide access to interesting stories / papers/ articles/ interviews relating to information warfare and cyberterrorism. For example, we re-enact an NPR interview with Richard Clarke relating to cyberterrorism. One article in the coursepack discusses the implications of the 2007 attack on Estonia's Internet infrastructure for the future of information warfare and cyberterrorism (Lesk [27]).

The course then moves on to a discussion of protection technologies, including intrusion detection systems, intrusion prevention systems and firewalls. On occasion, we have been able to get guest speakers from industry to talk about protection technologies (like Snort and Firewalls). One class is devoted to an animated discussion of computer immunology inspired by the paper by Stephanie Forrest and her co-authors [28]. Some students really get "turned on" to the ideas in this classic paper. (This author uses the term "classic" to refer to any paper in Computer Science that is at least ten years old and is still being read. Professors in Literature and other disciplines have a different take on what makes a piece of writing "classic".)

Finally, we move on to a discussion of "hot topics". In recent years, the focus has been on biometrics. According to a recent CSI/FBI survey (2006), biometrics was one of the fastest growing areas in terms of protective measures in computer security. We discuss biometrics in general [29] and face recognition technology in particular [30]. We also discuss RFID devices and the security and ethical issues raised by RFID chip implants for our culture [31]. Another fascinating paper that the author has included in his coursepack in the "hot topics" section relates to creating a certification authority for ISPs (see Parameswaran et al. [32]). ISPs would be certified by the CA only if their policies regarding outgoing and incoming mail satisfied certain criteria. The hot topics section of the course ends with a new assignment (that is, an assignment given for the first time this semester, spring 2009). For this assignment students are expected to present stories from the news, security-related news stories that appeared in the media during the current semester. This new assignment is described in Section IV.

The course ends with team presentations. Each team is responsible for giving a thirty minute presentation on a topic they choose from a long list of possible topics. Frequently chosen topics include intellectual property (especially music downloading), cyberterrorism, social engineering, and computer crime. These presentations usually use PowerPoint slides, but occasionally students create videos that present their topic in a creative manner. One team showed a video (in which the author appeared as a co-star) in which students hack into a professor's computer in order to change their grades in a computer security course. In addition to their dramatic presentation, the students presented some excellent technical material about how the poor professor could have been misled and (one might say, victimized) by social engineering and hacking.

III. TOPICS INTERLACED WITH NEWS STORIES

The author devotes several minutes of just about every class to news stories that relate to the issues covered in the course. Sometimes, these news stories are like "bulletins," that is, breaking news stories that appeared in the media on the day of the class or just a day or two before the class. At other times the news stories are fairly recent and significant events that occurred during the past few years. Almost always, the news story relates to the specific subject matter of the class for that day. However, if there is a big, breaking news story, the author will communicate this news to the class, even if it does not relate to the specific topic being covered on that day. However, all of the news stories relate to topics in the course.

The news stories communicate how important the topic of Information Assurance is for citizens at the beginning of the twenty-first century. The news stories (along with the wonderful Blown to Bits book by Abelson, Ledeen and Lewis [20]) has convinced the author that students in the modern era need to be aware of these security issues. Colleges and universities should view Information Assurance as a critical subject for students, just like writing, speaking and mathematics.

The author uses a collection of sources for the latest news stories. These include (but are not limited to):

- Dark reading (darkreading.com)
- Threat Level – Wired Blogs (blog.wired.com/27bstroke6/)
- Google News (technology section)
- ComputerWorld (computerworld.com/securitytopics/security)
- The Washington Post, Brian Krebs, Security Fix journalist (voices.washingtonpost.com/securityfix)
- The New York Times (nytimes.com/pages/technology)

Links to these sources are provided to students on Blackboard. This will help students to complete their "hot topics in the news" assignment that is described in the next section.

The author's teaching materials (the materials that he drags to class) are in folders that usually include a collection of news stories. He draws upon these news stories either at the very beginning of the class (e.g., for a hot news bulletin) or at that point in the class where the news story is especially relevant. For just about each section of the course, he has a collection of news stories relevant to that portion of the course.

The news stories change from semester to semester. Here are some news stories that come to mind from the last year or so:

- The Storm worm
- The case of Jamie Thomas who was fined $220,000 for illegal music downloading and subsequent decisions in that case
- How spam volume dramatically fell when a specific ISP was shut down
- RIAA, digital rights management, and other music industry news
- Phishing becomes spear phishing using information available on social networking sites
- Phishing became whaling when phishers targeted some really big fish (okay, so a whale is not really a fish) using fake federal court subpoenas.
- Information warfare operations involving the Russia / Georgia conflict
- The prevalence of Russian hackers in the new cybercrime environment
- Prosecutions, convictions relating to botnet creators
- Hacking incidents at the Pentagon that were evidently traced back to China
- New episodes of Web site defacement
- Proposed Anti-UCITA legislation in Massachusetts (four states already have such legislation)
- Flash drives for sale at an Afghani pawn shop are found to contain sensitive US military information
- Jihadist web sites brought down by a Lebanese US Citizen who now lives in Boston
- Jihadist web sites spreading information about cyberterrorism and other terrorist acts
- Social network security incidents
- Privacy issues relating to search engines and social networking sites
- Recurring news stories about huge breaches and loss of sensitive information (usually, relating to credit cards)
- Privacy issues relating to the USA Patriot Act and surveillance
- Search engine optimizer (SEO) emerging as a new profession. People are paying SEOs big bucks to improve their image on the Web.
- Depression among anti-virus vendors as they face new types of attacks

The author has collected many news stories over the past few semesters that related to issues in this course. He prints out these stories and saves them in folders that he can refer to during the course of the semester. From the author's perspective, the interesting and provocative nature of these stories illustrates how important issues in Information Assurance are in this day and age.

Bruce Schneier begins his book, Secrets and Lies [33], with a story about how he decided to keep track of criminal incidents on the Web during March of 2000. That is, he wanted to keep track of what were basically news stories for an entire month. After six days, his list of incidents (including a separate list of new vulnerabilities that were exposed and Web site defacements) became so over-whelming that he decided to stop this project.

During the spring and fall semesters of 2007 (several weeks during each of these semesters) this author tried to do something similar in nature, but a bit less ambitious. The idea was to print out and keep a folder of interesting news stories (as opposed to all news stories) relating to topics in his computer security and ethics course. Like Schneier he found that his collection of stories became huge. Here is just a small sample of the headlines from the many dozens of news stories that the author printed from 2007 :

- **China flexes muscles of its 'informationised' army**. Focus is on hacking incidents against the Pentagon. Source: The Guardian (UK)
- **The cyberwar against America.** Discusses information warfare operations of Al Qaeda and China, as well as the implications of the Estonia attacks that happened a few months earlier. Source: International Herald Tribune.
- **FBI Data Mining Went Beyond Targets**. Detailed article about surveillance techniques being used by the FBI (under the USA Patriot Act) to track "communities of interest". Source: The New York Times.
- **That e-mail from the IRS? It's not from the IRS.** Phishing scheme. Source: MSNBC
- **The Hand That Controls the Sock Puppet Could Get Slapped.** Cognitive hacking. Source: The New York Times.
- **How to Eliminate Spyware to Protect Your Business.** Source: Washington Post.
- **New Weapon in Web War Over Piracy.** Content recognition software. Intellectual property. Source: The New York Times
- **To Fight Identity Theft, a Call for Banks to Disclose Incidents.** Source: The New York Times.

- **Study Finds Web Antifraud Measure Ineffective.** Identity theft. Two factor authentication. Source: The New York Times.
- **In Web Uproar, Antipiracy Code Spreads Wildly.** Intellectual property. Bypassing copy protection on Blue-ray and HD-DVD disks. Source: The New York Times.
- **MySpace to Discuss Effort to Customize Ads.** Privacy. Source: The New York Times.
- **After Storm Worm, a flood of spam.** Computer Crime. Source: CNN.

Again, this is just a tiny sampling of the articles that the author printed out and it illustrates the fact that there is a nearly constant flow of news stories relating to the basic topics in this course. Furthermore, many of these news stories are quite interesting and provocative and they represent the kind of information that citizens in our culture should be able to understand.

The next section of this paper describes two assignments that the author is using for the first time this semester (spring 2009), assignments that relate to information assurance issues in the news.

IV. HOT TOPICS IN THE NEWS - ASSIGNMENTS

The course now devotes an entire class to news stories that are relevant to the course. This class occurs towards the end of the semester, just before the team presentations begin. On the first day of class, students are given the new "hot topics in the news" assignment. This assignment asks students to come to class on the designated day (again, near the end of the semester) with a news story that relates to a topic covered in our course. Each student is to come to class prepared to present the news story, like a journalist on CNN. Given the size of the class (and the length of time we have), we probably won't be able to call on every student to present their news story. We will have to decide on some mechanism to decide which students will do the verbal presentations. However, all students are required to submit their written news story, regardless of whether they do the in-class verbal presentation of not.

One option is to have the students submit their news stories using the Blackboard Digital Dropbox. This would allow the author to choose a dozen or so of the most interesting stories to present in class. In any event, all students are responsible for writing up a news story and also for providing the sources they used for their story. This is the first time the author has used this assignment in the course, but by the time the Colloquium occurs in June, he will have feedback on how the assignment worked out.

Students have various options for their final exams. One option is to do a take-home essay exam. Another option is to write a paper on a practical experience using some security tool (defensive, not offensive). A third option is to submit a term paper based on research they have done on a topic that interests them. This semester the author is adding a fourth option, which asks students to keep track of news relating to a specific area in Information Assurance that interests them. They are to keep print-outs of those news stories (maybe 4-5 stories each week) and they are to write brief summary descriptions for each of these stories.

In addition, they are to keep an "Information Assurance journal". This is a personal journal (with entries several times a week) that records their personal reactions to what they are learning from this news tracking exercise (and also, from our class, in general). Possible personal reactions would include things like:

- What the general public needs to know about this issue in information assurance,
- how public policies might address these issues,
- how computing professionals might address these issues, and
- how the general public can get educated about these issues.

This assignment (as written in the handout to the students) concludes as follows: "An important aspect of the journal is to record how your ideas relating to these topics are evolving. What impact is your focus on news stories in security having on your attitude towards these issues? At the end of the semester, conclude your journal with a summary of the impact this project has had on your attitude towards issues in computer security." If some students choose to do this final exam option (and if this paper is accepted for the Colloquium), the author will share the observations these students included in their computer security journals with his colleagues at the Colloquium.

These two assignments account for the "and Notes" part of the title of this paper. Students are to submit notes relating to the news stories. Those notes should be especially interesting among students who choose to write the Information Assurance journal.

V. CONCLUSIONS

The author describes a course that covers many topics of great interest to the general public, including computer crime, privacy, intellectual property, information warfare, social engineering, protective measures and biometrics. The news abounds with stories relating to these topics day after day. This paper describes how the author integrates news stories into his lecture materials. It also describes two new assignments that he is using this semester to encourage students to pay attention to the news and to become aware of the social implications of the issues discussed in this course.

VI. REFERENCES

[1] Available at the CSI web site www.gocsi.com.

[2] Tavani, Herman T., Ethics and Technology, John Wiley and Sons, 2003, 400 pp.

[3] Cranor, Lorrie Faith, "P3P: Making Privacy Policies More Useful," IEEE Security and Privacy, November / December 2003, pp. 40-48.

[4] Reiter, Michael K., and Rubin, Aviel D., "Anonymous Web Transactions with Crowds," CACM, February 1999, pp. 50-55.

[5] Available at www.torproject.org/.

[6] Siau, Keng, Nah, Fiona Fui-Hoon, and Teng, Limei, "Acceptable Internet Use Policy," CACM, January 2002, pp. 75-79.

[7] Mitnick, Kevin D., The Art of Deception, John Wiley Publishing, Indianapolis, 2002, 352 pp.

[8] Garber, Lee, "Melissa Virus Creates a New Type of Threat," IEEE Computer, June 1999, pp. 16-19.

[9] Berghel, Hal, "The Code Red Worm," CACM, December 2001, pp. 15-19.

[10] Bailey, Michael, Cooke, Evan, Jachanian, Farnan, Watson, David, and Nazario, Jose, "The Blaster Worm: Then and Now," IEEE Security and Privacy, July / August 2005, pp. 26-31.

[11] Smith, Brad, "A Storm (Worm) Is Brewing," IEEE Computer, February 2008, pp. 20-22.

[12] Chen, Thomas M., Jean-Marc, Robert, "Worm Epidemics in High-Speed Networks," IEEE Computer, June 2004, pp. 48-53.

[13] Heyman, Karen, "New Attack Tricks Antivirus Software," IEEE Computer, May 2007, pp. 18-20.

[14] McGraw, Gary and Hoglund, Greg, "Online Games and Security," IEEE Security and Privacy, September / October 2007, pp. 76-79.

[15] Pfleeger, Shari Lawrence, and Bloom, Gabrielle, "Canning Spam: Proposed Solutions to Unwanted Email," IEEE Security and Privacy, March / April 2005, pp. 40-47.

[16] Grimes, Galen A., "Compliance with the CAN-SPAM Act of 2003," CACM, February 2007, pp. 56-62.

[17] Geer, David, "Security Technologies Go Phishing," IEEE Computer, June 2005, pp. 18-21.

[18] Jagatic, Tom N., Johnson, Nathaniel A., Jakobsson, Markus, and Menczer, Filippo, "Social Phishing," CACM, October 2007, pp. 94-100.

[19] Ames, Wes, "Understanding Spyware: Risk and Response," IEEE IT Professional, September / October 2004, pp. 25-29.

[20] Abelson, Hal, Ledeen, Ken, and Lewis, Harry, Blown to Bits: Your Life, Liberty and Happiness After the Digital Explosion, Addison-Wesley, Reading, MA, 2008, 384 pp.

[21] Naumovich, Gleb and Memon, Nasir, "Preventing Piracy, Reverse Engineering and Tampering," IEEE Computer, July 2003, pp. 64-71.

[22] Thelander, Michael, "The Great Wall Syndrome," IEEE IT Professional, September / October 2005, pp. 25-30.

[23] Gyongyi, Zoltan and Garcia-Molina, Hector, "Spam: It's Not Just for Inboxes Anymore," IEEE Computer, October 2005, pp. 28-34.

[24] Cybenko, George, Giani, Annarita and Thompson, Paul, "Cognitive Hacking: A Battle for the Mind," IEEE Computer, August 2002, pp. 50-56.

[25] West, Ryan, "The Psychology of Security," CACM, April 2008, pp. 34-41.

[26] Denning, Dorothy E., Information Warfare and Security, Addison-Wesley, Reading, MA, 1999, 522 pp.

[27] Lesk, Michael, "The New Front Line," IEEE Security and Privacy, July / August 2007, pp. 76-79.

[28] Forrest, Stephanie, Hofmeyr, Steven, and Somayaji, Anil, "Computer Immunology," CACM, October 1997, pp. 88-96.

[29] Prabhakar, Salil, Pankanti, Sharath, and Jain, Anil K., "Biometric Recognition: Security and Privacy Concerns," IEEE Security and Privacy, March / April 2003, pp. 33-42.

[30] Bowyer, Kevin W., "Face Recognition Technology: Security versus Privacy," IEEE Technology and Society Magazine, Spring 2004, pp. 9-20.

[31] Foster, Kenneth R., and Jaeger, Jan, "RFID Inside: The Murky Ethics of Implanted Chips," IEEE Spectrum, March 2007, pp. 24-29.

[32] Parameswaran, Manoj, Zhao, Xia, Whinston, Andrew B., and Fang, Fang, "Reengineering the Internet for Better Security," IEEE Computer, January 2007, pp. 40-44.

[33] Schneier, Bruce, Secrets and Lies: Digital Security in a Networked World, John Wiley, 2004, 448 pp.